

NCC 督促電信事業精進商業簡訊風險管控機制，公私協力從源頭堵詐

為防堵商業簡訊成為詐騙管道，國家通訊傳播委員會（NCC）持續與內政部警政署、電信事業合作，公私協力實施商業簡訊涉詐攔阻措施，針對帶有網址及電話號碼之商業簡訊，於發送前，須預先審核登錄上開資料後，始可發送。

NCC 說明，該會統計今年 1 月至 10 月仍有 40 萬餘則惡意簡訊被成功發出，可能造成民眾財產損失。因此依「詐欺犯罪危害防制條例」第 14 條第 2 項規定，要求電信事業持續精進商業簡訊風險管控機制，簡訊內容如有超連結及電話號碼要進行檢查；NCC 預計 113 年 11 月 18 日起實施以下精進措施：

- 一、所有商業簡訊發送前，內容均須通過檢查，如帶有 URL、短網址或電話號碼，經查與企業登錄資料不符或未登錄者，則不予發送。
- 二、企業發送商業簡訊，若其內容有 URL、短網址或電話，皆需預先提出申請，經電信事業審核通過後，登錄 URL、短網址及電話號碼等企業專屬專用資料，後續

發送商業簡訊如有上開內容時，皆須與登錄資料相

符始可發送；如登錄資料變更時，亦需重新提出申請。

三、受信任之企業客戶經電信事業審核通過，可列入綠色

通道，不執行網址及聯絡電話偵測。

NCC 呼籲，民眾收到簡訊如帶有 URL、短網址或電話號碼，要小心求證，避免直接點擊簡訊內超連結或提供個資。如有疑慮可向內政部警政署「165」全民反詐騙網站或專線詢問。